PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-048478

(43)Date of publication of application : 18.02.2000

---

(51)Int.Cl. G11B 20/10

---

(21)Application number : 10-192084 (71)Applicant : YAMAHA CORP

(22)Date of filing : 07.07.1998 (72)Inventor : MATSUMOTO SEIJI
FURUKAWA MASAMICHI

---

(30)Priority
Priority number : 10161361
Priority date : 26.05.1998
Priority country : JP

---

(54) DIGITAL COPY CONTROL METHOD, AND DEVICE USING THE METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To clearly decide whether or not a digital recording medium is a authorized one by discriminating it with the presence of copy control information, electronic watermark information and error information of a specified pattern, reproducing only the data of authorized disks and recording only the proper data.

SOLUTION: A player 1 executes mutual certification processing of whether or not respective equipments are operated as an intention of a contents former between a display device 2 and a recorder 3 prior to reproduce a DVD. The certification with a limit using a common key is formed between the player 1 and the recorder 3, and only the recordable and reproducible contents are data transferred. The data on a bus 7 are ciphered so that the data transfer is validated only between the certified equipments. Further, the player 1 verifies whether or nor the DVD 8 to be reproduced is a legal medium by three kinds of information recorded on the DVD 8, that is, the copy control information, the electronic watermark information and the error information of the specified pattern.

LEGAL STATUS [Date of request for examination] 24.12.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration] withdrawal
[Date of final disposal for application] 20.09.2006
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] Two or more digital devices are connected through a bus, and perform authentication processing mutually between these digital devices, and the interface with which transmission and reception of digital data are performed only between the attested devices is minded. It faces transmitting the digital data from a digital recording medium to a receiving-side device from a transmitting-side device. A transmitting-side device and a receiving-side device So that a disapproval copy may be prevented based on the contents of the copy management information for the copy limit included in said digital data In the digital copy control approach of performing playback of the transmitting-side device concerned and a receiving-side device, and a limit of record actuation of operation Said copy management information which shows a copy restriction level is added to parts other than an image and/or voice among the Maine data recorded on said digital recording medium. Moreover, while adding digital-watermarking information to the parts of an image and/or voice among said Maine data The error information of a specific pattern is intentionally added to record data after adding an error correction code to said Maine data. The justification of the digital recording medium reproduced by said transmitting-side device is identified by the existence of said copy management information, digital-watermarking information, and the error information of a specific pattern. The digital copy control approach characterized by only for the data of a just digital recording medium performing the playback, and only suitable data recording them.

[Claim 2] In the digital recording medium by which it comes to record the Maine data playback or in order to record separately to said Maine data The copy management information rewritten so that said copy restriction level may be strengthened by the digital copy, when restricting a digital copy, while a copy restriction level is shown in parts other than an image and/or voice is contained. The digital-watermarking information which is not rewritten by the digital copy, either is included in parts other than an image and/or voice in the condition in which read-out outside is possible. Moreover, besides said Maine data The medium mark which is not read outside is added. These copy management information, digital-watermarking information, and a medium mark The digital recording medium characterized by being constituted so that the medium playback management and medium copy management by the side of the implementer of said Maine data to mean may be made with the combination of the contents of these three kinds of information.

[Claim 3] A watermark information addition means to add the digital-watermarking information which does not spoil the description to original data, A copy management information addition means to add the copy management information for restricting a copy to original data, An error correction code generation means to generate an error correction code from the Maine data with which said digital-watermarking information and copy management information were added to original data, and to add, Digital

recording medium production equipment characterized by having an error addition means to add the error of a specific pattern to the data to which the error correction code was added with this error correction code generation means as a medium mark.
[Claim 4] The interface with which authentication processing is mutually performed among two or more digital devices connected through the bus, and transmission and reception of digital data are performed only between the attested devices is minded. In the digital regenerative apparatus used as said transmitting-side device of the system which transmits digital data to a receiving-side device from a transmitting-side device The read-out means which reads record data from a digital recording medium, and the error detection correction means which extracts an error correction code from the read-out data read with this read-out means, and carries out detection correction of the error of read-out data based on this error correction code, A specific pattern error detection means to detect that the error detected with this error detection correction means is a specific pattern, An output means to output the data by which the error correction was carried out with said error detection correction means to said bus with the gestalt of the digital information suitable for the specification of said interface, A copy management information judging means to identify and judge the copy management information for restricting the digital copy included in said data by which the error correction was carried out, It has a digital-watermarking information judging means to identify and judge the digital-watermarking information which shows a copy restriction level from said data by which the error correction was carried out. Based on the detection result of said specific pattern error detection means, said digital recording medium judges an original medium or a copy medium. This judgment result, The digital regenerative apparatus characterized by being based on the judgment result in said copy management information judging means and said digital-watermarking information judging means, and permitting or forbidding playback of the data of said transmitting-side device.
[Claim 5] Said copy management information judging means discriminates a copy free-lancer and three kinds of copy restriction levels of that an one-generation copy is possible or the ban on a copy from said copy management information. Said digital-watermarking information judging means A copy free-lancer or two kinds of copy restriction levels of the ban on a copy are discriminated from said digital-watermarking information. Said specific pattern error detection means The digital regenerative apparatus according to claim 4 characterized by identifying the existence of the error of said specific pattern, judging whether it is the disk recorded on normal from the discernment result in each [these] means, and playing only the disk of normal.
[Claim 6] The digital regenerative apparatus according to claim 5 characterized by performing playback actuation when the error of a specific pattern is detected by said

specific pattern error detection means, and it is judged with an one-generation copy being possible with a copy management information judging means and it is judged with digital-watermarking information being the ban on a copy with a digital-watermarking information judging means.

[Claim 7] By the case where the error of a specific pattern is detected by said specific pattern error detection means, and the judgment result of said copy management information judging means and said digital-watermarking information judging means When it is the contents which carry out phase conflict except for the case where an one-generation copy of copy management information is possible, and digital-watermarking information serves as a ban on a copy, Or the digital regenerative apparatus according to claim 4 or 5 characterized by not reproducing when the error of a specific pattern is detected by the error detection means of said specific pattern, and when said digital-watermarking information is not able to be detected.

[Claim 8] The digital regenerative apparatus according to claim 4 or 5 characterized by not reproducing when the error of a specific pattern is not detected by the error detection means of said specific pattern, and when the judgment results of said copy management information judging means and said digital-watermarking information judging means differ.

[Claim 9] The interface with which authentication processing is mutually performed among two or more digital devices connected through the bus, and transmission and reception of digital data are performed only between the attested devices is minded. In the digital recording equipment used as said receiving-side device of the system which transmits digital data to a receiving-side device from a transmitting-side device While a copy free-lancer, and that an one-generation copy is possible or said copy management information which shows three kinds of copy restriction levels of the ban on a copy is added to parts other than an image and/or voice An one-generation copy of an image, and/or that a copy is possible into an audio part or the copy management information which receives the digital data with which two kinds of digital-watermarking information on the ban on a copy was added and which was received and identified is possible. And it is digital recording equipment characterized by recording digital-watermarking information as it is when the identified digital-watermarking information is the ban on a copy, and rewriting and recording only copy management information on the ban on a copy.

[Claim 10] The device constituted possible [an output] as an analog signal through said interface by said attested device in the digital data contents recorded on the digital recording medium, And the device constituted possible [record to a new digital recording medium] through said interface in the data contents inputted with an analog signal is included. In case all the these-attested devices carry out digital recording of the data contents supplied with an analog signal or a digital signal to a digital recording medium While being constituted so that the electronic authentication signature data

which can be attested only between the attested devices concerned may be recorded on the medium concerned in addition to data contents In case the digital data contents recorded on the digital recording medium are reproduced The digital copy control approach according to claim 1 characterized by being controlled to reproduce the digital data contents of the medium concerned only when it is detected and attested whether the electronic authentication signature data which can be attested only between said attested devices exist on the medium concerned.

[Claim 11] The digital recording medium according to claim 2 by which the electronic authentication signature data which can be attested only between the attested devices are characterized by the thing which it comes to record further.

[Claim 12] It is the digital regenerative apparatus according to claim 4 characterized by having further a means to forbid playback of data when electronic authentication signature data are not attested with a means to detect the electronic authentication signature data which can be attested only between the attested devices.

[Claim 13] Said some of attested devices [at least] are constituted possible [an output] as an analog signal through said interface in the digital data contents recorded on the digital recording medium. In case digital recording of the data contents supplied with these analog signals is carried out to a digital recording medium Digital recording equipment according to claim 9 characterized by being constituted so that the electronic authentication signature data which can be attested only between the attested devices concerned may be recorded on the medium concerned in addition to data contents.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Accepting especially a digital copy restrictively about the digital copy control approach in the system to which digital devices, such as a DVD (digital video disc) record regenerative apparatus, a digital video tape recorder, and digital one TV, were connected through the interface equipped with the mutual recognition function, this invention relates to the digital copy control approach and

the equipment using it in order to prevent effectively the disapproval copy which a data production person does not mean.

[0002]

[Description of the Prior Art] Before, digital recording playback devices, such as optical disk regenerative apparatus, such as DVD, and digital one TV, a digital video tape recorder, are mutually connected through the IEEE1394 bus which is an intelligent interface, and the system which transmits and receives the contents of an image or music between these digital devices is proposed. A user can prevent carrying out the disapproval copy which the production person of an image and a music content does not mean by checking whether it is that to which each device operates as an intention of a contents implementer, and forbidding a data transfer in this system, if it is the device which does not operate as an intention in case digital data is transmitted and received by devices.

[0003] In the digital Maine data transmitted, the copy management information called CCI (Copy Control Information) is contained. CCI consists of 2 bits, freely, a copy good and "10" show a copy good, and "11" shows ["00"] a copy failure only once.

[0004] When transmitting digital data, a transmitting-side device checks whether it is that to which a receiving-side device operates as an intention of a contents implementer on an IEEE1394 bus while checking the copy restriction level of contents by CCI first. If full authentication of a receiving-side device and the transmitting-side device is carried out, contents will be enciphered and transmitted from a transmitting-side device. In this case, when the CCI information on the contents from a transmitting-side device is "10", and when a receiving-side device is a sound recorder machine, CCI is rewritten and recorded on "11" after a copy. Future copies will be forbidden by this and a time cost copy will be realized.

[0005] On the other hand, the method using the digital-watermarking information called a watermark is also proposed as an option for preventing the disapproval copy of a digital visual equipment. This method is spaced through the place which is not [wave / image] conspicuous, the direct guide peg of the information is carried out, or is spaced through the specific frequency component of the frequency-conversion information on the HARASHIN number, and embeds information. By giving information that a copy is possible / improper to this watermark, assignment of C etc. is freely attained by only a copy good and playback.

[0006]

[Problem(s) to be Solved by the Invention] However, the conventional copy control approach using CCI enables it comparatively simply to rewrite "10" to "00" (for a copy to be freely possible) by the actuation which is 2 bits, in case CCI is rewritten by the receiving-side device from "10" (a copy is possible once) to "11" (a copy is impossible). For this reason, there is a problem that a disapproval copy is easy.

[0007] Moreover, since watermark information is distributed by the comparatively

large range concerning the image and voice in the Maine data, the approach of using a watermark cannot rewrite this easily by the receiving-side device. If it is going to rewrite this on user level, it must have a quite large-scale circuit. For this reason, it is effective in that a disapproval copy is prevented rather than CCI. However, since rewriting of a watermark cannot be performed simply, it cannot take easily the mode of rewriting a flag like [at the time of using CCI conversely], and permitting a copy only once.

[0008] This invention was made in view of such a trouble, and it aims at offering the equipment using the digital copy control approach and it which can prevent more effectively the digital copy which is not permitted, making possible the mode which restricts a copy.

[0009]

[Means for Solving the Problem] The digital copy control approach concerning this invention Two or more digital devices are connected through a bus, and perform authentication processing mutually between these digital devices, and the interface with which transmission and reception of digital data are performed only between the attested devices is minded. It faces transmitting the digital data from a digital recording medium to a receiving-side device from a transmitting-side device. A transmitting-side device and a receiving-side device So that a disapproval copy may be prevented based on the contents of the copy management information for the copy limit included in said digital data In what performs playback of the transmitting-side device concerned and a receiving-side device, and a limit of record actuation of operation Said copy management information which shows a copy restriction level is added to parts other than an image and/or voice among the Maine data recorded on said digital recording medium. Moreover, while adding digital-watermarking information to the parts of an image and/or voice among said Maine data The error information of a specific pattern is intentionally added to record data after adding an error correction code to said Maine data. It is characterized by identifying the justification of the digital recording medium reproduced by said transmitting-side device by the existence of said copy management information, digital-watermarking information, and the error information of a specific pattern, and only for just disc data performing the playback, and recording only suitable data.

[0010] To said Maine data of the digital recording medium concerning this invention The copy management information rewritten so that said copy restriction level may be strengthened by the digital copy, when restricting a digital copy, while a copy restriction level is shown in parts other than an image and/or voice is contained. The digital-watermarking information which is not rewritten by the digital copy, either is included in parts other than an image and/or voice in the condition in which read-out outside is possible. Moreover, besides said Maine data The medium mark which is not read outside is added. These copy management information, digital-watermarking

information, and a medium mark It is characterized by being constituted so that the medium playback management and medium copy management by the side of the implementer of said Maine data to mean may be made with the combination of the contents of these three kinds of information.

[0011] The digital recording medium production equipment concerning this invention A watermark information addition means to add the digital-watermarking information which does not spoil the description to original data, A copy management information addition means to add the copy management information for restricting a copy to original data, An error correction code generation means to generate an error correction code from the Maine data with which said digital-watermarking information and copy management information were added to original data, and to add, It is characterized by having an error addition means to add the error of a specific pattern to the data to which the error correction code was added with this error correction code generation means as a medium mark.

[0012] Moreover, the interface with which authentication processing is mutually performed among two or more digital devices connected through the bus, and transmission and reception of digital data are performed only between the attested devices is minded. The digital regenerative apparatus concerning this invention used as said transmitting-side device of the system which transmits digital data to a receiving-side device from a transmitting-side device The read-out means which reads record data from a digital recording medium, and the error detection correction means which carries out detection correction of the error of the read-out data read with this read-out means, A specific pattern detection means to detect that the error detected with this error detection correction means is a specific pattern, An output means to output the data by which the error correction was carried out with said error correction means to said bus with the gestalt of the digital information suitable for the specification of said interface, A copy management information judging means to identify and judge the copy management information for restricting the digital copy included in said data by which the error correction was carried out, It has a digital-watermarking information judging means to identify and judge the digital-watermarking information which shows a copy restriction level from said data by which the error correction was carried out. Based on the detection result of the error detection means of said specific pattern, said digital recording medium judges an original medium or a copy medium. This judgment result, By the judgment result in said copy management information judging means and said digital-watermarking information judging means, it is characterized by performing activation or prohibition of playback actuation.

[0013] In one concrete mode of this invention, as information currently recorded into the record medium Said copy management information has either condition of a copy free-lancer and three kinds of copy restriction levels of that an one-generation copy

is possible or the ban on a copy. Said digital-watermarking information takes either a copy free-lancer or two kinds of copy restriction levels of the ban on a copy. It is characterized by enabling it to identify the disk of normal, as the condition of whether it is related with the error of said added specific pattern or there is nothing is taken and it can judge whether it is the disk recorded on normal in the combination of each [these] signal.

[0014] In other concrete modes of this invention, when the error of a specific pattern is detected by said specific pattern detection means, and it is judged with an one-generation copy being possible with a copy management information judging means and it is judged with digital-watermarking information being the ban on a copy with a digital-watermarking information judging means, it is characterized by performing playback actuation.

[0015] In the concrete mode of further others of this invention, by the case where the error of a specific pattern is detected by said specific pattern detection means, and the judgment result of said copy management information judging means and said digital-watermarking information judging means When it is the contents which carry out phase conflict except for the case where an one-generation copy of copy management information is possible, and digital-watermarking information serves as a ban on a copy, Or when the error of a specific pattern is detected by said specific pattern error detection means, and when said digital-watermarking information is not able to be detected, it is characterized by not reproducing.

[0016] In the concrete mode of further others of this invention, when the error of a specific pattern is not detected by said specific pattern error detection means, and when the judgment results of said copy management information judging means and said digital-watermarking information judging means differ, it is characterized by not reproducing.

[0017] Furthermore, the digital recording equipment concerning this invention The interface with which authentication processing is mutually performed among two or more digital devices connected through the bus, and transmission and reception of digital data are performed only between the attested devices is minded. In the digital recording equipment used as said receiving-side device of the system which transmits digital data to a receiving-side device from a transmitting-side device While a copy free-lancer, and that an one-generation copy is possible or said copy management information which shows three kinds of copy restriction levels of the ban on a copy is added to parts other than an image and/or voice An one-generation copy of an image, and/or that a copy is possible into an audio part or the copy management information which receives the digital data with which two kinds of digital-watermarking information on the ban on a copy was added and which was received and identified is possible. And when the identified digital-watermarking information is the ban on a copy, it is characterized by recording digital-watermarking information as it is, and

rewriting and recording only copy management information on the ban on a copy.

[0018] According to this invention, the justification of a digital recording medium is judged using three kinds of information. The 1st information is the copy management information which shows the copy restriction level contained in parts an image and other than voice among the Maine data, and when restricting a digital copy, if copied, it will be rewritten so that a copy restriction level may be strengthened. The 2nd information is the digital-watermarking information which is similarly included in the parts of an image and voice among the Maine data, and shows a copy restriction level, this information is not rewritten even if a digital copy is carried out, and rewriting is very difficult. The 3rd information is the error information (it is hereafter called a medium mark) of the specific pattern intentionally added to the data after an error correction, and since it is added out of the Maine data, this information is not included in the Maine data reproduced from the record medium, but if a digital copy is carried out, it will disappear.

[0019] Thus, since three information has a property different, respectively, it can judge in a detail whether it is that to which the digital recording medium was justly copied by the condition of these three information. That is, first, since it will disappear if the digital copy of the medium mark is carried out once, it can judge an original medium or a copy medium by the existence of a medium mark. Moreover, although both copy management information and digital-watermarking information show a copy restriction level, freely, in the case of the medium for which a digital copy is good, only the combination of each of copy management information and digital-watermarking information which shows copy C freely is effective, and since others may have been rewritten without copy management information passing through processing of normal, the medium by which a medium mark is not detected can be recognized to be the medium which is not just. Moreover, when copy management information and digital-watermarking information must show a copy restriction level when [both] it permits a copy under a certain limit, and either shows copy C freely, this is also the medium which is not just. Furthermore, when each of copy management information and digital-watermarking information shows a predetermined copy restriction level, only copy management information is rewritten by the copy, but even if it is intentionally rewritten at this time so that copy management information may fall or present condition maintain a copy restriction level, this is recognized by disappearance of a medium mark and it can judge with it being the medium which is not just.

[0020] Since a transmitting-side device forbids playback of digital data when it is presumed by the transmitting-side device as a result of such a judgment that it is the medium which is not just, the medium can perform neither playback nor record, but, thereby, can prevent a disapproval copy effectively. Moreover, since digital data is transmitted to the attested receiving-side device so that it may become possible

[only playback] possible [record playback] according to the copy restriction level when it has been recognized as a transmitting-side device being a just medium, the digital copy under the restricted conditions is also attained.

[0021] Moreover, it attests only between the devices these-attested also when it was possible to carry out digital recording via an analog signal between the attested devices, and ******** electronic authentication signature data are recorded with digital data contents, and if playback of data contents is permitted only when this authentication is materialized further in addition to the recognition technique mentioned above, the disapproval copy of the data contents itself can be prevented more certainly.

[0022]

[Embodiment of the Invention] Hereafter, the gestalt of desirable implementation of this invention is explained with reference to a drawing. Drawing 1 is the block diagram showing the digital data transceiver structure of a system concerning one example of this invention. The DVD player 1 which is a transmitting-side device, and the display unit 2 and the DVD recorder 3 which is a receiving-side device are mutually connected through each interfaces 4, 5, and 6 and bus 7 based on an IEEE1394 specification. The DVD player 1 transmits the digital data which reproduced DVD8 with which the image and the music content used as the transmitting source were recorded, and was obtained to a display 2 and a recorder 3 through a bus 7. A recorder 3 records the digital data which restricted when it was the digital data with which the digital copy is permitted, and was received on DVD9.

[0023] A player 1 performs [whether it is the device by which each / these / device operates between a display unit 2 and a recorder 3 as an intention of a contents implementer, and] mutual recognition processing in advance of playback of DVD8. Since there is no record function in a display unit 2, the full authentication which used the public key is materialized between players 1. In this case, data will be transmitted if the contents to which record is forbidden are also reproducible. Between a player 1 and a recorder 3, the authentication with a limit which used the common key is materialized. In this case, data transfer only of the contents for which record and playback are also good is carried out. The data on a bus 7 are enciphered so that data transfer may become effective only between the attested devices.

[0024] Moreover, a player 1 verifies whether DVD8 which it is going to reproduce is a just medium by three kinds of information currently recorded on DVD8, i.e., CCI, (copy management information), the watermark (digital-watermarking information), and the media mark (medium mark: error information of a specific pattern).

[0025] Drawing 2 is the block diagram showing the configuration of the original recording production equipment which produces the original recording of DVD with which these information was added. The HARASHIN number which should be recorded is the watermark adjunct 11, and embeds a watermark at the part into which the

HARASHIN number is not conspicuous, for example, the big part of a brightness difference with a masking effect etc. Moreover, you may make it a watermark embed the HARASHIN number in the specific frequency of the signal which carried out the Fourier transform. Although compression coding of the signal with which the watermark was embedded is carried out by the encoder 12, it is either of the processes so far, and 2-bit CCI which a production person means is added by the CCI addition means which the interior does not illustrate. Here, CCI is added with the encoder 12. Next, after ID and an error detection code are added by the ID/EDC adjunct 13, an error correction code is added in the ECC generation section 14. The data with which the error correction code was added can be borne at about 1% of reading error. Here, the error information of a specific pattern is added to extent which does not exceed such an error rate as a media mark with the error addition means 15. That is, a bit error is produced intentionally. The pattern or the pattern on a frequency shaft on a time-axis is sufficient as a media mark. The data with which the media mark was added are the eight-to-fourteen modulation section 16, and 8->16 (DVD) or 8->14 (CD) modulation of them is carried out, and they are recorded on the original recording disk 18 by the record driver 17. DVD produced by this original recording 18 serves as the original version.

[0026] Drawing 3 is the block diagram showing the detail of the player 1 of drawing 1 . After the record data recorded on DVD8 being read by the read head 21 and getting over in the EFM recovery section 22, error correction processing is made in the ECC recovery section 23. The media mark detection section 24 searches for the inclination of the error pattern in the ECC recovery section 23 by a correlation operation etc., and when the error has occurred by the specific pattern decided beforehand, it judges with those with a media mark. The output from the media mark detection section 24 is supplied to the output-control section 26. The data to which it restored in the ECC recovery section 23 are supplied to a decoder 25 through the CCI judging section 28 and the watermark judging section 27. The watermark judging section 27 and the CCI judging section 28 judge the watermark extracted, respectively and CCI, and output a judgment result to the output-control section 26. In addition, you may make it judge in but [not in signal decode processing] the front, or the back depending on recording methods, such as a watermark. The output-control section 26 is controlled to supply the Maine data which contain a watermark and CCI from a decoder 25 and which should be transmitted to I/F29, when it is judged from the judgment result of the detection output of the media mark detection section 24, the watermark judging section 27, and the CCI judging section 28 that data transmission is possible. Moreover, in forbidding playback of a player, it controls the playback control section 31 if needed. And when data are supplied to I/F29, the Maine data which should be transmitted are changed into the fixed bit rate based on IEEE1394, and are outputted on a bus 7.

[0027] Since it is in the condition which a recorder 3 can copy on the other hand when the Maine data have been transmitted, the digital copy of this is carried out, but when copy C is shown only under the limit with the watermark contained in the Maine data, and CCI, it rewrites so that a restriction level may go up CCI to a copy and coincidence.

[0028] Drawing 4 is the table showing good/failure of the media mark and watermark which the output-control section 26 judges, CCI and playback, and record. Since the media mark is not included in the Maine data which should be transmitted as mentioned above, it does not exist in a copy disk. Moreover, naturally it is not contained in the old disk of DVD or CD. For this reason, the disk with which a media mark exists can be judged to be an original disk, and the disk not existing can be judged to be a copy disk or the old disk.

[0029] A watermark is set as "11", when restricting "00" and a copy, in permitting a copy freely. CCI presupposes freely that a copy is impossible at a copy good and "11" only once by "00" a copy good and "10." When a watermark does not exist, since it is the old disk, the combination of those with a media mark is contradictory without a watermark. Therefore, it considers as an invalid (it is not just) irrespective of the pattern of CCI in this case. Moreover, when there are not both a media mark and a watermark, since it is the old disk, let only copy C (10) and playback be C (11) only copy C (00) and once freely according to CCI.

[0030] When both a watermark and CCI are "00", since a copy is good, record and playback are freely permitted irrespective of the existence of a media mark. However, since conflict arises when a watermark is [CCI] "10" or "11" in "00", it thinks that intentional bit manipulation was made and considers as the disk which is not just.

[0031] Since it is a copy with a limit when a watermark is "11", CCI is set to "10" or "11." Therefore, when CCI is "00", it is dealt with with the disk which is not just. Since only 1 time must be an original disk at the time of copy C (10), only when there is a media mark, it is effective, and CCI judges with the disk which rewrote CCI intentionally and carried out it and which is not just, when there is nothing. Since it is the ban on a copy when CCI is "11", only playback is made good.

[0032] Since neither playback nor record is permitted when it judges that DVD8 is the disk which is not just by the above decision, a player 1 does not transmit the Maine data to a display unit 2 and a recorder 3. Moreover, when only playback is judged to be good, the Maine data are transmitted to a display unit 2 and a recorder 3, but since the data has CCI only with playback, the recorder 3 which is the configuration that authentication can be received does not perform record actuation.

[0033] In addition, the view of this playback and propriety control of record agrees not only to the digital data transmission system shown in the example but to the system of digital playback / record device by transmission using the analog signal which existed from the former well. For example, since a watermark is put in when an analog

input is used as the input source, as shown in drawing 4 , if it considers in that case that media mark nothing and CCI apply to a watermark, it can process like this invention. Moreover, if it regards as those with a media mark with the registered digital broadcast wave being receivable in inputting a digital broadcast wave, since a next watermark and CCI can also be given satisfactory at all, it can process like this invention.

[0034] Moreover, two or more digital devices which were explained previously are connected through a bus. Even if it is a digital data transmission system through the interface with which authentication processing is mutually performed between these digital devices, and transmission and reception of digital data are performed only between the attested devices If recorded on a just medium, that voice and/or the contents of playback of an image can be outputted as an analog signal, and possibility that digital recording will be again carried out to another record medium about this output using the device or the illegal device of not attesting other than the attested device remains. Such a record medium in an authentication device system as the medium of the old system without a watermark or a media mark -- not recognizing, if it does not obtain but it is recorded that a copy free-lancer or an one-generation copy of the CCI is still more nearly possible When this medium is carried in between authentication device systems once again, not to mention playback, based on CCI for which an one-generation copy is good, a copy medium will be again created with the authentication device system itself, and a just medium may be made from the medium which is not just. Of course, forbidding analog output entirely cannot be carried out, and also giving encryption (encryption) to analog output and including a decryption circuit in all the image display units that are in all playback side devices in the world cannot be realized in practice, either.

[0035] What is necessary is just to constitute so that additional use of the electronic authentication signature data which can be recognized only between these authentication device systems in the record and/or playback actuation in the attested device may be carried out in order to prevent from reproducing the medium which was created using such a non-attesting device and which is not just by the attested device. This becomes possible [whether it is what the record data of that medium were justly recorded on within the authentication device system being able to check, and controlling activation of playback and/or record actuation by this electronic authentication signature on it] between authentication device systems. therefore, even if it is going to reproduce the medium data which were recorded using the non-attesting device and which are not just by the device of either of the authentication device systems, the electronic authentication signature which should be performed between authentication device systems does not exist, or the authentication result of an electronic authentication signature becomes abortive, and Use of the medium which is not just can preventing-**** by being made to perform

playback actuation in this case .

[0036] Although various data encryption methods can be used about generation and authentication of an electronic authentication signature, the example using what applied for example, the public-key-encryption-ized method here is explained. A RSA (Rivest, Shamir, Adleman) code typical as a public-key-encryption-ized method sets the basis of safety to the difficulty of a large number of factorization in prime numbers, and performs encryption/decryption processing by count of a exponentiation remainder. An encryption procedure is expressed with "the C=E(M) = (e-th power of M) remainder n", and a decryption procedure is expressed with "M=D(C) = (d-th power of C) remainder n." Here, M is a plaintext and C is a cipher. e, n, and the decryption key of an encryption key are d and n, and the encryption key e and the common key n are exhibited, and make the decryption key d secret. The decision of Keys e, d, and n is made in the following procedure. (1) Choose the two big prime factors p and q as arbitration, and consider as n=pq. The least common multiple L of (2), (p-1), and (q-1) is calculated, it is as relatively prime as L and the integer e of arbitration smaller than L is searched for. (3) Ask for d which fills the ed=1 remainder L. In this way, as for the selected values e, d, and n, "remainder (ed ** of M) n=M" is materialized to all the plaintexts M. Although a decode person has to know the decryption key d to decode Cipher C, for that purpose, and (p-1) (q-1) needs to get to know the secret prime factors p and q, and it is necessary to calculate "the 1st [-] power remainder L of d=e" from the least common multiple L and a public key e, and to ask for a private key d. Since a public key n is the product of the prime factors p and q, it does not become a code for the integer which is extent which can carry out factorization in prime numbers of the public key n easily. Then, p and q are usually made into 100-figure each (decimal number) extent, and the public key n is made into about 200 figures. If it carries out like this, even if it uses a 1000MIPS computer, it will become this calculation to factorization in prime numbers for millions years, and decode is substantially impossible.

[0037] Actuation of the device in a concrete authentication device system is explained. The common key n is first memorized beforehand by each device in an authentication device system. In case these devices are written in through the data contents which should be recorded, within a device, they encipher the contents which combined the device recognition ID of self, and the proper ID of the contents which should be recorded with the encryption key e currently exhibited, create them as data of an electronic authentication signature, and are recorded on a medium with the data contents which should record this. Only when it decrypts using a common key and an external secret secret decryption key, and it confirms Device ID and data content ID, in operating this medium by the device of either of the authentication device systems, and being just is admited, it controls to reproduce this. If this data medium is recorded by the non-attesting device, there are no data of an electronic authentication

signature, or it will become the thing (the specific encryption which is common between authentication device systems is not made) of decryption impossible, it will have, and this will not be accepted to be a just medium, and such data contents will not be reproduced.

[0038]

[Effect of the Invention] According to this invention, as stated above, it can judge clearly whether it is what has a just digital recording medium by combining the information on three kinds of different properties, and the effectiveness that the digital copy which is not just can be prevented more effectively is done so, making possible the mode which restricts a copy by this.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram of the digital data transmission system concerning one example of this invention.

[Drawing 2] It is the block diagram of the original recording production equipment of the disk which applied this invention.

[Drawing 3] It is the detail block diagram of the player of the system of drawing 1 .

[Drawing 4] It is drawing showing the good/improper correspondence relation between three kinds of information used by this invention, record, and playback.

[Description of Notations]

1 [-- An interface, 7 / -- Bus.] -- A player, 2 -- A display unit, 3 -- A recorder, 4, 5, 6

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－48478
（P2000－48478A）
(43)公開日　平成12年２月18日(2000.2.18)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ　５Ｄ０４４

審査請求　未請求　請求項の数13　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－192084

(22)出願日　平成10年７月７日(1998.7.7)

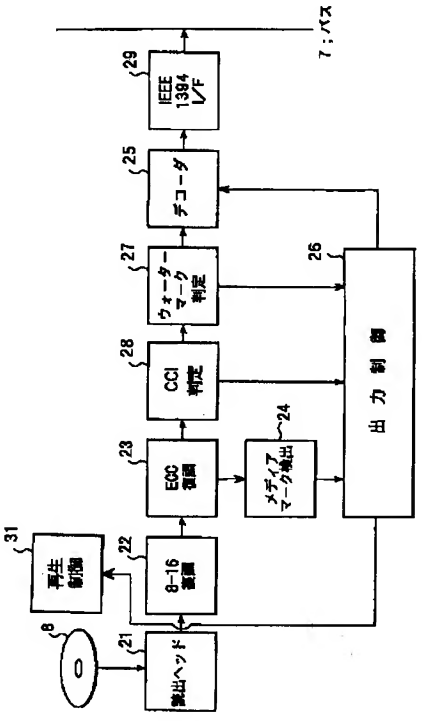
(31)優先権主張番号　特願平10－161361
(32)優先日　平成10年５月26日(1998.5.26)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004075
ヤマハ株式会社
静岡県浜松市中沢町10番１号
(72)発明者　松本　誠二
静岡県浜松市中沢町10番１号　ヤマハ株式会社内
(72)発明者　古川　雅通
静岡県浜松市中沢町10番１号　ヤマハ株式会社内
(74)代理人　100092820
弁理士　伊丹　勝

Ｆターム(参考)　5D044 AB05 AB07 BC01 BC02 CC03
CC04 DE50 DE68 EF05 FG18
GK17 HL08 HL11

(54)【発明の名称】　ディジタルコピー制御方法及びそれを用いた装置

(57)【要約】
【課題】　コピーを制限する態様を可能にしつつ、許可されないディジタルコピーをより効果的に防止する。
【解決手段】　３種類の情報によってディジタル記録媒体の正当性を判定する。第１の情報は、メインデータの映像・音声以外の部分に含まれるコピー制限レベルを示すコピー管理情報で、ディジタルコピーを制限する場合、コピーされるとコピー制限レベルが強化されるように書き替えられる。第２の情報は、同じくメインデータの映像・音声の部分に含まれてコピー制限レベルを示す電子透かし情報で、この情報はディジタルコピーされても書き替えられないし、書き換えは極めて困難である。第３の情報は、エラー訂正後のデータに意図的に付加される特定パターンのエラー情報（媒体マーク）で、この情報は、メインデータ外に付加されるものであるから、記録媒体から再生されたメインデータには含まれず、ディジタルコピーされると消失する。



【特許請求の範囲】

【請求項１】　バスを介して複数のディジタル機器が接続され、これらディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタル記録媒体からのディジタルデータを送信するに際し、送信側機器および受信側機器は、前記ディジタルデータに含まれるコピー制限のためのコピー管理情報の内容に基づいて不許可コピーを防止するように、当該送信側機器および受信側機器の再生および記録動作の動作制限を行うディジタルコピー制御方法において、

前記ディジタル記録媒体に記録されるメインデータのうち映像及び／又は音声以外の部分にコピー制限レベルを示す前記コピー管理情報を付加し、また前記メインデータのうち映像及び／又は音声の部分に電子透かし情報を付加すると共に、前記メインデータにエラー訂正コードを追加した後の記録データに特定パターンのエラー情報を意図的に付加し、

前記送信側機器で再生されるディジタル記録媒体の正当性を、前記コピー管理情報、電子透かし情報、及び特定パターンのエラー情報の有無により識別して、正当なディジタル記録媒体のデータのみその再生を行い、また適切なデータのみ記録することを特徴とするディジタルコピー制御方法。

【請求項２】　再生または別途記録するためにメインデータが記録されてなるディジタル記録媒体において、

前記メインデータには、映像及び／又は音声以外の部分にコピー制限レベルを示すとともにディジタルコピーを制限する場合ディジタルコピーによって前記コピー制限レベルを強化するように書き替えられるコピー管理情報が含まれ、また、映像及び／又は音声以外の部分にはディジタルコピーによっても書き替えられない電子透かし情報とが外部に読み出し可能な状態で含まれ、

前記メインデータ外には、外部に読み出されない媒体マークが付加され、

これらコピー管理情報、電子透かし情報、および媒体マークは、これら３種類の情報の内容の組み合わせによって前記メインデータの作成者側の意図するところの、媒体再生管理および媒体コピー管理がなされるように構成されていることを特徴とするディジタル記録媒体。

【請求項３】　原データにその特徴を損なわない電子透かし情報を付加する透かし情報付加手段と、

原データにコピーを制限するためのコピー管理情報を付加するコピー管理情報付加手段と、

原データに前記電子透かし情報及びコピー管理情報が付加されたメインデータからエラー訂正コードを生成して付加するエラー訂正コード生成手段と、

このエラー訂正コード生成手段でエラー訂正コードが付加されたデータに特定パターンのエラーを媒体マークとして付加するエラー付加手段とを備えたことを特徴とするディジタル記録媒体作製装置。

【請求項４】　バスを介して接続された複数のディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタルデータを送信するシステムの前記送信側機器として用いられるディジタル再生装置において、

ディジタル記録媒体から記録データを読み出す読出手段と、

この読出手段で読み出された読出データからエラー訂正コードを抽出し、このエラー訂正コードに基づいて読出データの誤りを検出訂正する誤り検出訂正手段と、

この誤り検出訂正手段で検出された誤りが特定パターンであることを検出する特定パターン誤り検出手段と、

前記誤り検出訂正手段で誤り訂正されたデータを前記インタフェースの仕様に合ったディジタル情報の形態で前記バスに出力する出力手段と、

前記誤り訂正されたデータに含まれるディジタルコピーを制限するためのコピー管理情報を識別して判定するコピー管理情報判定手段と、

前記誤り訂正されたデータからコピー制限レベルを示す電子透かし情報を識別して判定する電子透かし情報判定手段とを備え、

前記特定パターン誤り検出手段の検出結果に基づいて前記ディジタル記録媒体がオリジナル媒体かコピー媒体かを判定し、この判定結果と、前記コピー管理情報判定手段及び前記電子透かし情報判定手段での判定結果とに基づいて前記送信側機器のデータの再生を許可又は禁止するようにしたことを特徴とするディジタル再生装置。

【請求項５】　前記コピー管理情報判定手段は、前記コピー管理情報からコピーフリー、１世代コピー可又はコピー禁止の３種類のコピー制限レベルを識別し、

前記電子透かし情報判定手段は、前記電子透かし情報からコピーフリー又はコピー禁止の２種類のコピー制限レベルを識別し、

前記特定パターン誤り検出手段は、前記特定パターンの誤りの有無を識別し、

これら各手段での識別結果から正規に記録されたディスクであるかどうかを判定して正規のディスクのみ再生するようにしたことを特徴とする請求項４記載のディジタル再生装置。

【請求項６】　前記特定パターン誤り検出手段で特定パターンの誤りが検出され、コピー管理情報判定手段で１世代コピー可と判定され、且つ電子透かし情報判定手段で電子透かし情報がコピー禁止であると判定された場合、再生動作を実行することを特徴とする請求項５記載のディジタル再生装置。

【請求項７】　前記特定パターン誤り検出手段で特定パターンの誤りが検出された場合で且つ前記コピー管理情

報判定手段と前記電子透かし情報判定手段の判定結果が、コピー管理情報が１世代コピー可で且つ電子透かし情報がコピー禁止となっている場合を除いて相矛盾する内容となっているとき、又は前記特定パターンの誤り検出手段で特定パターンの誤りが検出された場合で且つ前記電子透かし情報が検出出来なかった場合、再生を行わないことを特徴とする請求項４又は５記載のディジタル再生装置。

【請求項８】　前記特定パターンの誤り検出手段で特定パターンの誤りが検出されなかった場合で且つ、前記コピー管理情報判定手段と前記電子透かし情報判定手段の判定結果が異なる場合、再生を行わないことを特徴とする請求項４又は５記載のディジタル再生装置。

【請求項９】　バスを介して接続された複数のディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタルデータを送信するシステムの前記受信側機器として用いられるディジタル記録装置において、

映像及び／又は音声以外の部分にコピーフリー、１世代コピー可又はコピー禁止の３種類のコピー制限レベルを示す前記コピー管理情報が付加されると共に、映像及び／又は音声の部分にコピー可又はコピー禁止の２種類の電子透かし情報が付加されたディジタルデータを受信する受信し、

識別されたコピー管理情報が１世代コピー可で、且つ識別された電子透かし情報がコピー禁止である場合、電子透かし情報はそのまま記録し、コピー管理情報のみコピー禁止に書き換えて記録することを特徴とするディジタル記録装置。

【請求項１０】前記認証された機器には、ディジタル記録媒体に記録されたディジタルデータコンテンツを前記インターフェースを介することなくアナログ信号として出力可能に構成された機器、及びアナログ信号で入力されるデータコンテンツを前記インターフェースを介することなく新たなディジタル記録媒体に記録可能に構成された機器を含み、これら認証された機器の全ては、アナログ信号またはディジタル信号で供給されるデータコンテンツをディジタル記録媒体にディジタル記録する際に、当該媒体上にデータコンテンツに加えて当該認証された機器間でのみ認証可能な電子認証署名データを記録するように構成されると共に、

ディジタル記録媒体に記録されたディジタルデータコンテンツを再生する際に、当該媒体上に前記認証された機器間でのみ認証可能な電子認証署名データが存在するか否かを検出し、

認証された場合のみ当該媒体のディジタルデータコンテンツを再生するように制御されることを特徴とする請求項１記載のディジタルコピー制御方法。

【請求項１１】認証された機器間でのみ認証可能な電子認証署名データが、更に記録されてなることを特徴とする請求項２記載のディジタル記録媒体。

【請求項１２】認証された機器間でのみ認証可能な電子認証署名データを検出する手段と、電子認証署名データが認証されなかった場合はデータの再生を禁止する手段とを、更に有することを特徴とする請求項４記載のディジタル再生装置。

【請求項１３】前記認証された機器の少なくとも一部は、ディジタル記録媒体に記録されたディジタルデータコンテンツを前記インターフェースを介することなくアナログ信号として出力可能に構成されており、

これらアナログ信号で供給されるデータコンテンツをディジタル記録媒体にディジタル記録する際に、データコンテンツに加え当該認証された機器間でのみ認証可能な電子認証署名データを当該媒体上に記録するように構成されることを特徴とする請求項９記載のディジタル記録装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ＤＶＤ（ディジタル・ビデオ・ディスク）記録再生装置、ディジタルＶＴＲ、ディジタルＴＶ等のディジタル機器が相互認証機能を備えたインタフェースを介して接続されたシステムにおけるディジタルコピー制御方法に関し、特にディジタルコピーを制限的に認めつつ、データ作製者の意図しない不許可コピーを効果的に防止するためディジタルコピー制御方法及びそれを用いた装置に関する。

【０００２】

【従来の技術】従来より、ＤＶＤ等の光ディスク再生装置やディジタルＴＶ、ディジタルＶＴＲ等のディジタル記録再生機器をインテリジェントなインタフェースであるＩＥＥＥ１３９４バスを介して相互に接続し、これらディジタル機器間で映像や音楽のコンテンツを送受信するシステムが提案されている。このシステムでは、機器同士でディジタルデータを送受信する際に、それぞれの機器がコンテンツ作成者の意図どおりに動作するものかを確認し、意図どおりに動作しない機器であればデータの転送を禁止することにより、ユーザが映像・音楽コンテンツの作製者の意図しない不許可コピーをしてしまうのを防止することができる。

【０００３】伝送されるディジタルのメインデータの中には、ＣＣＩ（Copy Control Information）と呼ばれるコピー管理情報が含まれている。ＣＣＩは２ビットからなり、“００”が自由にコピー可、“１０”が１回だけコピー可、“１１”がコピー不可を示す。

【０００４】ディジタルデータを送信するとき、送信側機器は、まずＣＣＩによってコンテンツのコピー制限レベルを確認すると共に、ＩＥＥＥ１３９４バス上で受信側機器がコンテンツ作成者の意図どおりに動作するものかどうかを確認する。受信側機器と送信側機器が完全認

証されたら送信側機器からコンテンツが暗号化されて送信される。この場合、送信側機器からのコンテンツのＣＣＩ情報が例えば“１０”の場合でかつ受信側機器が録音機器の場合には、コピー後にＣＣＩを“１１”に書き替えて記録する。これによって、以後のコピーは禁止され、一世代コピーが実現されることになる。

【０００５】一方、ディジタル映像機器の不許可コピーを防止するための別の方法として、ウォーターマークと呼ばれる電子透かし情報を用いる方式も提案されている。この方式は、映像波形などの目立たないところに透かし情報を直接足し込んだり、原信号の周波数変換情報の特定の周波数成分に透かし情報を埋め込むようにしたものである。このウォーターマークにコピー可／不可の情報を与えておくことにより、自由にコピー可、再生のみ可等の指定が可能になる。

【０００６】

【発明が解決しようとする課題】しかしながら、ＣＣＩを用いた従来のコピー制御方法では、受信側機器でＣＣＩを例えば“１０”（１回のみコピー可）から“１１”（コピー不可）に書き替える際に、“１０”を“００”（自由にコピー可）に書き替えることが２ビットの操作で比較的簡単に可能になる。このため、不許可コピーが容易であるという問題がある。

【０００７】また、ウォーターマークを使用する方法は、透かし情報がメインデータ中の映像・音声に係る比較的広い範囲に分散されるため、受信側機器でこれを簡単に書き替えることはできない。ユーザレベルでこれを書き替えようとすると、かなり大規模な回路を備えなければならない。このため、ＣＣＩよりも不許可コピーを防止する点で効果がある。しかしながら、ウォーターマークの書き換えは簡単にできないため、逆にＣＣＩを用いた場合のようにフラグを書き替えてコピーを１回だけ許可するという態様を簡単に採ることができない。

【０００８】この発明は、このような問題点に鑑みなされたもので、コピーを制限する態様を可能にしつつ、許可されないディジタルコピーをより効果的に防止することができるディジタルコピー制御方法及びそれを用いた装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】この発明に係るディジタルコピー制御方法は、バスを介して複数のディジタル機器が接続され、これらディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタル記録媒体からのディジタルデータを送信するに際し、送信側機器および受信側機器は、前記ディジタルデータに含まれるコピー制限のためのコピー管理情報の内容に基づいて不許可コピーを防止するように、当該送信側機器および受信側機器の再生および記録動作の動作制限を行うものにおいて、前記ディジタル記録媒体に記録されるメインデータのうち映像及び／又は音声以外の部分にコピー制限レベルを示す前記コピー管理情報を付加し、また前記メインデータのうち映像及び／又は音声の部分に電子透かし情報を付加すると共に、前記メインデータにエラー訂正コードを追加した後の記録データに特定パターンのエラー情報を意図的に付加し、前記送信側機器で再生されるディジタル記録媒体の正当性を、前記コピー管理情報、電子透かし情報、及び特定パターンのエラー情報の有無により、識別して正当ディスクのデータのみその再生を行い、また適切なデータのみ録音することを特徴とする。

【００１０】この発明に係るディジタル記録媒体の前記メインデータには、映像及び／又は音声以外の部分にコピー制限レベルを示すと共にディジタルコピーを制限する場合ディジタルコピーによって前記コピー制限レベルを強化するように書き替えられるコピー管理情報が含まれ、また、映像及び／又は音声以外の部分にはディジタルコピーによっても書き替えられない電子透かし情報とが外部に読み出し可能な状態で含まれ、前記メインデータ外には、外部に読み出されない媒体マークが付加され、これらコピー管理情報、電子透かし情報、および媒体マークは、これら３種類の情報の内容の組み合わせによって前記メインデータの作成者側の意図するところの、媒体再生管理および媒体コピー管理がなされるように構成されていることを特徴とする。

【００１１】この発明に係るディジタル記録媒体作製装置は、原データにその特徴を損なわない電子透かし情報を付加する透かし情報付加手段と、原データにコピーを制限するためのコピー管理情報を付加するコピー管理情報付加手段と、原データに前記電子透かし情報及びコピー管理情報が付加されたメインデータからエラー訂正コードを生成して付加するエラー訂正コード生成手段と、このエラー訂正コード生成手段でエラー訂正コードが付加されたデータに特定パターンのエラーを媒体マークとして付加するエラー付加手段とを備えたことを特徴とする。

【００１２】また、バスを介して接続された複数のディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタルデータを送信するシステムの前記送信側機器として用いられるこの発明に係るディジタル再生装置は、ディジタル記録媒体から記録データを読み出す読出手段と、この読出手段で読み出された読出データのエラーを検出訂正する誤り検出訂正手段と、この誤り検出訂正手段で検出された誤りが特定パターンになっていることを検出する特定パターン検出手段と、前記誤り訂正手段で誤り訂正されたデータを前記インタフェースの仕様に合ったディジタル情報の形態で前記バスに出力する出力手段と、前記誤り訂正されたデータに含まれるディジタルコピー

を制限するためのコピー管理情報を識別して判定するコピー管理情報判定手段と、前記誤り訂正されたデータからコピー制限レベルを示す電子透かし情報を識別して判定する電子透かし情報判定手段とを備え、前記特定パターンの誤り検出手段の検出結果に基づいて前記ディジタル記録媒体がオリジナル媒体かコピー媒体かを判定し、この判定結果と、前記コピー管理情報判定手段及び前記電子透かし情報判定手段での判定結果により、再生動作の実行又は禁止を行うようにしたことを特徴とする。

【００１３】この発明の１つの具体的態様において、記録媒体中に記録されている情報として、前記コピー管理情報はコピーフリー、１世代コピー可又はコピー禁止の３種類のコピー制限レベルのいずれかの状態を持ち、前記電子透かし情報はコピーフリー又はコピー禁止の２種類のコピー制限レベルのいずれかを取り、前記追加された特定パターンの誤りに関しては有るか無いかのいずれかの状態を取り、これら各信号の組み合わせで正規に記録されたディスクであるかどうかを判定できるようにして、正規のディスクを識別できるようにしたことを特徴とする。

【００１４】この発明の他の具体的態様においては、前記特定パターン検出手段で特定パターンの誤りが検出され、コピー管理情報判定手段で１世代コピー可と判定され、且つ電子透かし情報判定手段で電子透かし情報がコピー禁止であると判定された場合、再生動作を実行することを特徴とする。

【００１５】この発明の更に他の具体的態様においては、前記特定パターン検出手段で特定パターンの誤りが検出された場合で且つ前記コピー管理情報判定手段と前記電子透かし情報判定手段の判定結果が、コピー管理情報が１世代コピー可で且つ電子透かし情報がコピー禁止となっている場合を除いて相矛盾する内容となっているとき、又は前記特定パターン誤り検出手段で特定パターンの誤りが検出された場合で且つ前記電子透かし情報が検出出来なかった場合、再生を行わないことを特徴とする。

【００１６】この発明の更に他の具体的態様においては、前記特定パターン誤り検出手段で特定パターンの誤りが検出されなかった場合で且つ、前記コピー管理情報判定手段と前記電子透かし情報判定手段の判定結果が異なる場合、再生を行わないことを特徴とする。

【００１７】更に、この発明に係るディジタル記録装置は、バスを介して接続された複数のディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタルデータを送信するシステムの前記受信側機器として用いられるディジタル記録装置において、映像及び／又は音声以外の部分にコピーフリー、１世代コピー可又はコピー禁止の３種類のコピー制限レベルを示す前記コピー管理情報が付加されると共に、映像及び／又は音声の部分にコピー可又はコピー禁止の２種類の電子透かし情報が付加されたディジタルデータを受信する受信し、識別されたコピー管理情報が１世代コピー可で、且つ識別された電子透かし情報がコピー禁止である場合、電子透かし情報はそのまま記録し、コピー管理情報のみコピー禁止に書き換えて記録することを特徴とする。

【００１８】この発明によれば、３種類の情報によってディジタル記録媒体の正当性を判定する。第１の情報は、メインデータのうち映像・音声以外の部分に含まれるコピー制限レベルを示すコピー管理情報で、ディジタルコピーを制限する場合、コピーされるとコピー制限レベルが強化されるように書き替えられる。第２の情報は、同じくメインデータのうち映像・音声の部分に含まれてコピー制限レベルを示す電子透かし情報で、この情報はディジタルコピーされても書き替えられないし、書き換えは極めて困難である。第３の情報は、エラー訂正後のデータに意図的に付加される特定パターンのエラー情報（以下、媒体マークと呼ぶ）で、この情報は、メインデータ外に付加されるものであるから、記録媒体から再生されたメインデータには含まれず、ディジタルコピーされると消失する。

【００１９】このように、３つの情報がそれぞれ異なる性質を持っているので、これら３つの情報の状態によってディジタル記録媒体が正当にコピーされたものかどうかを詳細に判定することができる。即ち、まず、媒体マークは、１回ディジタルコピーされると消失するので、媒体マークの有無によって、それがオリジナル媒体かコピー媒体かが判定できる。また、コピー管理情報と電子透かし情報とは、共にコピー制限レベルを示すものであるが、自由にディジタルコピー可の媒体の場合、コピー管理情報と電子透かし情報とは、いずれも自由にコピー可を示す組合せのみ有効であり、その他はコピー管理情報が正規の処理を経ずに書き替えられた可能性があるので、媒体マークの検出されない媒体は正当でない媒体と認識することができる。また、ある制限の下にコピーを許容する場合には、コピー管理情報と電子透かし情報とが共にコピー制限レベルを示すものでなければならず、いずれか一方が自由にコピー可を示す場合には、これも正当でない媒体である。更に、コピー管理情報と電子透かし情報とがいずれも所定のコピー制限レベルを示す場合には、コピーによってコピー管理情報のみが書き替えられるが、このとき、コピー管理情報がコピー制限レベルを低下又は現状維持するように意図的に書き替えられても、媒体マークの消失によってこれが認識され、正当でない媒体であると判定することができる。

【００２０】送信側機器で、このような判定の結果、正当でない媒体であると認定された場合には、送信側機器がディジタルデータの再生を禁止するので、その媒体は、再生も記録もできず、これにより不許可コピーを効

果的に防止することができる。また、送信側機器が正当な媒体であると認識した場合には、そのコピー制限レベルに応じて記録再生可又は再生のみ可となるように、認証した受信側機器にディジタルデータを送信するので、制限された条件下でのディジタルコピーも可能になる。

【００２１】また、認証された機器間では、アナログ信号経由でディジタル記録することが可能な場合にも、これら認証された機器間でのみ認証し合あえる電子認証署名データをディジタルデータコンテンツと共に記録するようにし、上述した認識手法に加え、さらにこの認証が成立した場合にのみ、データコンテンツの再生を許可するようにすれば、データコンテンツそのものの不許可コピーをより確実に防止できる。

【００２２】

【発明の実施の形態】以下、図面を参照して、この発明の好ましい実施の形態について説明する。図１は、この発明の一実施例に係るディジタルデータ送受信システムの構成を示すブロック図である。送信側機器であるＤＶＤプレーヤ１と、受信側機器であるディスプレイ装置２及びＤＶＤレコーダ３は、ＩＥＥＥ１３９４仕様に準拠したそれぞれのインタフェース４，５，６及びバス７を介して相互に接続されている。ＤＶＤプレーヤ１は、送信ソースとなる映像・音楽コンテンツが記録されたＤＶＤ８を再生して得られたディジタルデータを、バス７を介してディスプレイ２及びレコーダ３に伝送する。レコーダ３は、ディジタルコピーが許可されているディジタルデータである場合に限り、受信したディジタルデータをＤＶＤ９に記録する。

【００２３】プレーヤ１は、ＤＶＤ８の再生に先立ち、ディスプレイ装置２及びレコーダ３との間でこれら各機器がコンテンツ作成者の意図どおりに動作する機器であるかどうか相互認証処理を実行する。例えば、例えばディスプレイ装置２には、記録機能が無いので、プレーヤ１との間には公開鍵を用いた完全認証が成立する。この場合、記録が禁止されているコンテンツでも再生が可であればデータが転送される。プレーヤ１とレコーダ３との間は、共通鍵を用いた制限付き認証が成立する。この場合、記録も再生も可であるコンテンツのみがデータ転送される。認証された機器間でのみデータ転送が有効となるように、バス７上のデータは暗号化される。

【００２４】また、プレーヤ１は、再生しようとするＤＶＤ８が正当な媒体であるかどうかを、ＤＶＤ８に記録されている３種類の情報、即ち、ＣＣＩ（コピー管理情報）、ウォーターマーク（電子透かし情報）及びメディアマーク（媒体マーク：特定パターンのエラー情報）によって検証する。

【００２５】図２は、これら情報が付加されたＤＶＤの原盤を作製する原盤作製装置の構成を示すブロック図である。記録すべき原信号は、ウォーターマーク付加部１１で、原信号の目立たない部分、例えばマスキング効果がある輝度差の大きな部分等に、ウォーターマークを埋め込む。また、ウォーターマークは、原信号をフーリエ変換した信号の特定の周波数に埋め込むようにしてもよい。ウォーターマークが埋め込まれた信号はエンコーダ１２によって圧縮符号化されるが、ここまでの過程のいずれかで、内部の図示しないＣＣＩ付加手段によって、作製者の意図する２ビットのＣＣＩが付加されている。ここではエンコーダ１２でＣＣＩを付加している。次にＩＤ／ＥＤＣ付加部１３でＩＤやエラー検出コードが付加された後、ＥＣＣ生成部１４でエラー訂正コードが付加される。エラー訂正コードが付加されたデータは、例えば１％程度の読み取りエラーに耐えられるものである。ここでは、そのようなエラーレートを超えない程度に、エラー付加手段１５によって特定パターンのエラー情報をメディアマークとして付加する。つまり意図的にビット誤りを生じさせる。メディアマークは、時間軸上のパターンでも周波数軸上でのパターンでもよい。メディアマークが付加されたデータは、ＥＦＭ変調部１６で、８→１６（ＤＶＤ）又は８→１４（ＣＤ）変調され、記録ドライバ１７によって原盤ディスク１８に記録される。この原盤１８によって作製されたＤＶＤがオリジナル版となる。

【００２６】図３は、図１のプレーヤ１の詳細を示すブロック図である。ＤＶＤ８に記録された記録データは、読出ヘッド２１によって読み出され、ＥＦＭ復調部２２で復調されたのち、ＥＣＣ復調部２３でエラー訂正処理がなされる。メディアマーク検出部２４は、ＥＣＣ復調部２３でのエラーパターンの傾向を相関演算等によって求め、予め決められた特定のパターンでエラーが発生している場合には、メディアマーク有りと判定する。メディアマーク検出部２４からの出力は出力制御部２６に供給される。ＥＣＣ復調部２３で復調されたデータは、ＣＣＩ判定部２８、ウォーターマーク判定部２７を経てデコーダ２５に供給される。ウォーターマーク判定部２７及びＣＣＩ判定部２８は、それぞれ抽出されたウォーターマーク及びＣＣＩを判定し、出力制御部２６に判定結果を出力する。なお、ウォーターマーク等の記録方式によっては、信号復号処理中ではなく、その前或いは後で判定するようにしても良い。出力制御部２６は、メディアマーク検出部２４の検出出力とウォーターマーク判定部２７及びＣＣＩ判定部２８の判定結果とから、データ伝送が可能と判断した場合、デコーダ２５からウォーターマーク及びＣＣＩを含む伝送すべきメインデータをＩ／Ｆ２９に供給するように制御する。また、プレーヤの再生を禁止する場合には、必要に応じて再生制御部３１を制御する。そしてＩ／Ｆ２９にデータが供給された場合には、伝送すべきメインデータはＩＥＥＥ１３９４に準拠する固定ビットレートに変換されてバス７上に出力される。

【００２７】一方、レコーダ３は、メインデータが伝送

されてきた場合には、コピー可の状態であるからこれをディジタルコピーするが、メインデータに含まれるウォーターマーク及びＣＣＩがある制限下でのみコピー可を示している場合には、コピーと同時にＣＣＩを制限レベルが上がるように書き替える。

【００２８】図４は、出力制御部２６が判断するメディアマーク、ウォーターマーク及びＣＣＩと再生及び記録の可／不可を示す表である。メディアマークは、上述したように、伝送すべきメインデータには含まれていないので、コピーディスクには存在しない。また、ＤＶＤやＣＤの旧ディスクにも当然含まれていない。このため、メディアマークが存在するディスクはオリジナルディスク、存在しないディスクはコピーディスク又は旧ディスクと判断することができる。

【００２９】ウォーターマークは、自由にコピーを許容する場合には“００”、コピーを制限する場合には“１１”に設定される。ＣＣＩは、“００”で自由にコピー可、“１０”で１回だけコピー可、“１１”でコピー不可とする。ウォーターマークが存在しない場合には、旧ディスクであるから、ウォーターマーク無しでメディアマーク有りという組合せは矛盾する。従って、この場合にはＣＣＩのパターンに拘わらず無効（正当でない）とする。また、メディアマーク、ウォーターマークが共に無い場合には、旧ディスクであるから、ＣＣＩに応じて自由にコピー可（００）、１回だけコピー可（１０）、再生のみ可（１１）とする。

【００３０】ウォーターマークとＣＣＩが共に“００”の場合には、自由にコピー可であるから、メディアマークの有無に拘わらず記録・再生を許可する。しかし、ウォーターマークが“００”で、ＣＣＩが“１０”又は“１１”の場合には、矛盾が生じるので、意図的なビット操作がなされたと考えて正当でないディスクとする。

【００３１】ウォーターマークが“１１”のときは制限付きコピーであるから、ＣＣＩは、“１０”又は“１１”となる。従って、ＣＣＩが“００”のときは、正当でないディスクと取り扱う。ＣＣＩが１回だけコピー可（１０）のときは、オリジナルディスクでなければならないので、メディアマークがある時のみ有効で、無いときにはＣＣＩを意図的に書き換えした正当でないディスクと判定する。ＣＣＩが“１１”のときには、コピー禁止であるから、再生のみ可とする。

【００３２】以上の判断により、ＤＶＤ８が正当でないディスクであると判定された場合には、再生も記録も許可しないので、プレーヤ１は、ディスプレイ装置２にもレコーダ３にもメインデータを伝送しない。また、再生のみ可と判断された場合には、ディスプレイ装置２、レコーダ３へメインデータを伝送するが、認証を受け得る構成であるレコーダ３は、そのデータが再生のみとのＣＣＩを有しているので、記録動作は行わない。

【００３３】なお、この再生及び記録の可否制御の考え方は、実施例に示したディジタルデータ伝送システムに限らず、従来から存在したアナログ信号を使った伝送によるディジタル再生・記録機器のシステムにも良く合致する。例えば、図４に示すように、入力ソースとしてアナログ入力が用いられた場合、ウォーターマークは入れられるので、その場合には、メディアマーク無し、且つＣＣＩはウォーターマークに準ずると見なせば、この発明と同様に処理できる。また、ディジタル放送波を入力する場合には、登録されたディジタル放送波を受信できていることをもってメディアマーク有りと見れば、後のウォーターマーク、ＣＣＩも全く問題なく付与できるので、この発明と同様に処理できる。

【００３４】また、先に説明したような、複数のディジタル機器がバスを介して接続され、これらディジタル機器間で相互に認証処理が行われ、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介するディジタルデータ伝送システムであったとしても、正当な媒体に記録されたものであればその音声及び／又は映像の再生内容をアナログ信号として出力でき、この出力について、認証された機器以外の非認証の機器または違法な機器を用い、再度別の記録媒体にディジタル記録されてしまう可能性が残る。このような記録媒体は、認証機器システムでは、ウォーターマーク、またはメディアマークを持たない旧システムの媒体として認識せざるを得ず、さらにはそのＣＣＩがコピーフリーまたは１世代コピー可と記録されていると、この媒体が今一度認証機器システム間に持ち込まれた場合、再生は勿論のこと、１世代コピー可のＣＣＩに基づいて、認証機器システム自体で再度コピー媒体を作成してしまうことになり、正当でない媒体から正当な媒体が作られてしまう可能性がある。アナログ出力を一切禁止することは勿論実施できるはずはなく、また、アナログ出力にエンクリプション（暗号化）を施すということも、再生側機器全てに、例えば世の中にある全ての映像ディスプレイ装置に暗号解読回路を組み込むことも実際上実現不可能である。

【００３５】このような非認証機器を用いて作成された正当でない媒体を、認証された機器で再生できないようにするには、認証された機器における記録及び／又は再生動作に、これら認証機器システム間でのみ認識できる電子認証署名データを追加利用するように構成すれば良い。これにより認証機器システム間ではこの電子認証署名により、その媒体の記録データが認証機器システム内で正当に記録されたものか否かが確認でき、そのうえで再生及び／又は記録動作の実行を制御することが可能となる。したがって、非認証の機器を用いて記録された、正当でない媒体データを認証機器システム内のいずれかの機器で再生しようとしても、認証機器システム間で行われるべき電子認証署名が存在しないか、または電子認証署名の認証結果が不成立となり、この場合には再生動

作を行わない様にする事によって、正当でない媒体の使用を防止できる。

【００３６】電子認証署名の生成・認証については、種々のデータ暗号化方式を利用できるが、ここでは例えば公開鍵暗号化方式を応用したものを利用した例を説明する。公開鍵暗号化方式として代表的なＲＳＡ（Rivest,Shamir,Adleman)暗号は大きな数の素因数分解の困難さに安全性の根拠をおき、べき乗剰余の計算により暗号化／復号化処理を行うものである。暗号化手順は「Ｃ＝Ｅ（Ｍ）＝（Ｍのｅ乗）剰余ｎ）」で表され、復号化手順は「Ｍ＝Ｄ（Ｃ）＝（Ｃのｄ乗）剰余 ｎ」で表される。ここで、Ｍは平文、Ｃは暗号文である。暗号化鍵はｅとｎ、復号化鍵はｄとｎで、暗号化鍵ｅと共通鍵ｎは公開し、復号化鍵ｄは秘密とする。鍵ｅ，ｄ，ｎの決定は次の手順で行う。（１）２つの大きな素数ｐ，ｑを任意に選び、ｎ＝ｐｑとする。（２）（ｐ－１）と（ｑ－１）の最小公倍数Ｌを計算し、Ｌと互いに素でＬより小さな任意の整数ｅを求める。（３）ｅｄ＝１剰余Ｌを満たすｄを求める。こうして選んだ値ｅ，ｄ，ｎは、全ての平文Ｍに対し、「（Ｍのｃｄ乗）剰余ｎ＝Ｍ」が成立する。解読者が暗号文Ｃを解読するには復号化鍵ｄを知らなければならないが、そのためには秘密の素数ｐ，ｑを知り、（ｐ－１）および（ｑ－１）の最小公倍数Ｌと公開鍵ｃとから「ｄ＝ｃの－１乗剰余Ｌ」を演算し、秘密鍵ｄを求める必要がある。公開鍵ｎは素数ｐおよびｑの積であるから公開鍵ｎが容易に素因数分解できる程度の整数では暗号にならない。そこで通常はｐとｑを各１００桁（十進数）程度とし、公開鍵ｎは２００桁程度としている。こうすれば、１０００ＭＩＰＳの電子計算機を用いても素因数分解に数百万年かかる勘定になり、実質的に解読は不可能である。

【００３７】具体的な認証機器システム内の機器の動作を説明する。まず認証機器システム内の各機器には予め共通鍵ｎが記憶されている。これら機器は記録すべきデータコンテンツを媒体に書き込む際に機器内で、自己の機器認識ＩＤおよび記録すべきコンテンツの固有ＩＤを組み合わせた内容を公開されている暗号化鍵ｅで暗号化して電子認証署名のデータとして作成し、これを記録すべきデータコンテンツと共に媒体に記録する。この媒体を認証機器システム内のいずれかの機器で動作させる場合には、共通鍵と外部非公開の秘密復号化鍵を用いて復号化し、機器ＩＤとデータコンテンツＩＤを確かめ、正当と認められる場合のみ、これを再生するように制御する。もしもこのデータ媒体が、非認証の機器により記録されたものであると、電子認証署名のデータがないか、あるいは、復号化不能のもの（認証機器システム間で共通する特定の暗号化がなされていないの）となり、もってこれを正当な媒体と認めることはなく、また、そのようなデータコンテンツは、再生されることはない。

【００３８】

【発明の効果】以上述べたように、この発明によれば、３種類の異なる性質の情報を組み合わせることにより、ディジタル記録媒体が正当なものかどうかを明確に判定することができ、これによりコピーを制限する態様を可能にしつつ、正当でないディジタルコピーをより効果的に防止することができるという効果を奏する。

【図面の簡単な説明】

【図１】　この発明の一実施例に係るディジタルデータ伝送システムのブロック図である。

【図２】　この発明を適用したディスクの原盤作製装置のブロック図である。

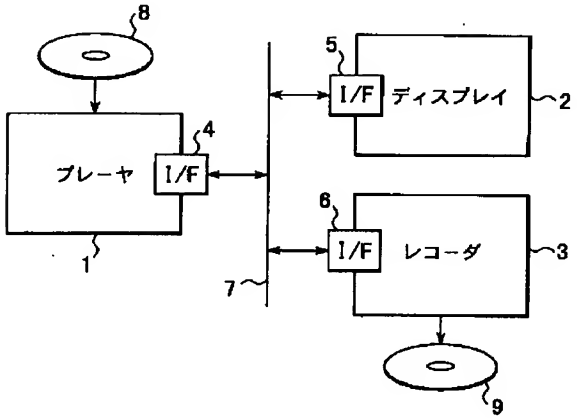
【図３】　図１のシステムのプレーヤの詳細ブロック図である。

【図４】　この発明で使用される３種類の情報と記録及び再生の可／不可の対応関係を示す図である。

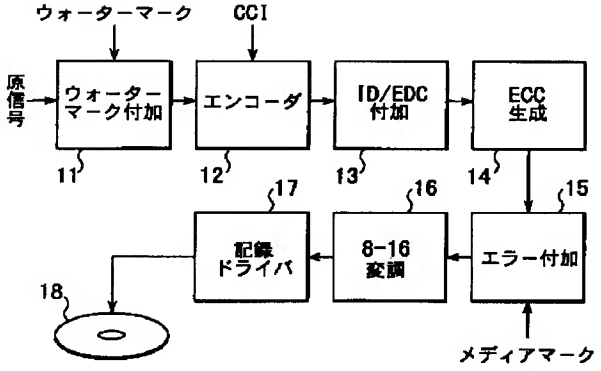
【符号の説明】

１…プレーヤ、２…ディスプレイ装置、３…レコーダ、４，５，６…インタフェース、７…バス。

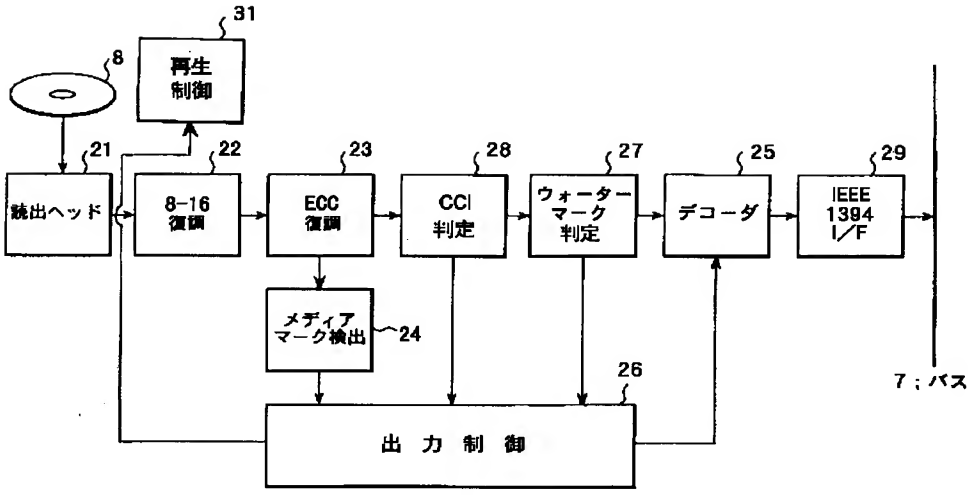
【図１】



【図２】



【図３】


31
再生制御
8
21
22
23
28
27
25
29
読出ヘッド
8-16復調
ECC復調
CCI判定
ウォーターマーク判定
デコーダ
IEEE 1394 I/F
メディアマーク検出
24
26
出力制御
7；バス

【図４】

入力の状態	入力コンテンツのフラグ		入力ソースの素性			再生コントロール	再生出力時のフラグ		録音コントロール	録音後		
	Water Mark	CCI	システム	正当性	概要		Water Mark	CCI		Water Mark	CCI	説明
メディアマーク有りディスク	11	11	新	正規	録音禁止	○	11	11	×	−	−	正規の録音禁止ディスク
	11	10	新	正規	一世代コピー可	○	11	10	○	11	11	正規の一世代コピー可のオリジナルディスク
	11	00	新	不正	不正改造	×			×	−	−	不正改造ディスク、新装置では再生不可能
	00	11	新	不正	不正改造	×			−	−	−	正規の組み合わせには無い
	00	10	新	不正	不正改造	×			−	−	−	正規の組み合わせには無い
	00	00	新	正規	コピーフリー	○	00	00	○	00	00	オリジナルのコピーフリーディスク
	無し	11	新	不正	不正改造	×			−	−	−	意味の無い組み合わせ（改造）
	無し	10	新	不正	不正改造	×			−	−	−	意味の無い組み合わせ（改造）
	無し	00	新	不正	不正改造	×			−	−	−	意味の無い組み合わせ（改造）
メディアマーク無しディスク := デジタル入力	11	11	新	正規	一世代コピー可ディスクのコピー	○	11	11	−	−	−	一世代コピー可のコンテンツの録音ディスク：不正コピーディスクの可能性有り
	11	10	新	不正	不正改造	×			×	−	−	不正コピーディスク
	11	00	新	不正	不正改造	×			×	−	−	不正コピーディスク
	00	11	新	不正	不正改造	×			×	−	−	意味の無い組み合わせ（改造）
	00	10	新	不正	不正改造	×			×	−	−	意味の無い組み合わせ（改造）
	00	00	新	正規	コピーフリーディスクのコピー	○	00	00	○	00	00	コピーフリーディスクのコピーディスク
	無し	11	旧	正規	コピー禁止	○	無し	11	×	無し	11	旧ディスクの為、不正防止は弱い（ＣＣＩのみ）
	無し	10	旧	正規	一世代コピー可	○	無し	10	○	無し	11	旧ディスクの為、不正防止は弱い
	無し	00	旧又は個人製作ディスク	正規	コピーフリー	○	無し	00	○	無し	00	旧ディスクの為、不正防止は弱い
アナログ入力	11	−	新	正規	コピー禁止	○	11	11*	×	−	−	アナログでもコピーコントロールが可能
	00	−	新	正規	コピーフリー	○	00	00*	○	00	00	アナログでもコピーコントロールが可能
	無し	−	旧ディスク又は個人製作ディスク	正規＋旧不正	１世代コピー可	○	無し	10*	○	無し	11	１世代のみコピー可とする。（ＳＣＭＳと同等）
放送波	11	11	新システム	正規	コピー禁止	○	11	11	×	−	−	基本的に不正信号は出てこない
	11	10	新システム	正規	一世代コピー可	○	11	10	○	11	11	基本的に不正信号は出てこない
	00	00	新システム	正規	コピーフリー	○	00	00	○	00	00	基本的に不正信号は出てこない
	無し	11	現状システム	正規	コピー禁止	○	無し	11	×	−	−	基本的に不正信号は出てこない
	無し	10	現状システム	正規	一世代コピー可	○	無し	10	○	無し	11	基本的に不正信号は出てこない
	無し	00	現状システム	正規	コピーフリー	○	無し	00	○	無し	00	基本的に不正信号は出てこない

11*，00*，10*は、それぞれ11，00，10として扱うという意味

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第４区分
【発行日】平成１７年９月２９日（２００５．９．２９）

【公開番号】特開２０００－４８４７８（Ｐ２０００－４８４７８Ａ）
【公開日】平成１２年２月１８日（２０００．２．１８）
【出願番号】特願平１０－１９２０８４
【国際特許分類第７版】
　G11B 20/10
【ＦＩ】
　G11B 20/10　　H

【手続補正書】
【提出日】平成１７年４月２７日（２００５．４．２７）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　バスを介して複数のディジタル機器が接続され、これらディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタル記録媒体からのディジタルデータを送信するに際し、送信側機器が、前記ディジタルデータに含まれるコピー制限のための情報の存否と内容とに基づいて不許可コピーを防止するように、当該送信側機器の再生動作もしくは記録動作の動作制限を行うディジタルコピー制御方法において、
　本来のディジタル記録媒体は、記録されるメインデータのうち映像及び／又は音声以外の部分にコピー制限レベルを示すコピー管理情報が付加されており、また前記メインデータのうち映像及び／又は音声の部分に電子透かし情報が付加されており、さらに前記メインデータにエラー訂正コードを追加した後の記録データに特定パターンのエラー情報が意図的に付加されて製造されており、
　前記送信側機器は、再生されるディジタル記録媒体を、前記コピー管理情報、前記電子透かし情報、及び前記特定パターンのエラー情報の有無と内容とにより、正当なディジタル記録媒体であるかないかを判断し、前記正当なディジタル記録媒体であると判断された場合は、その記録データを受信側機器へ送信する
　ことを特徴とするディジタルコピー制御方法。
【請求項２】
　バスを介して複数のディジタル機器が接続され、これらディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタル記録媒体からのディジタルデータを送信するに際し、送信側機器あるいは受信側機器が、前記ディジタルデータに含まれるコピー制限のための情報の存否と内容とに基づいて不許可コピーを防止するように、当該送信側機器あるいは受信側機器の再生動作もしくは記録動作の動作制限を行うディジタルコピー制御方法において、
　本来のディジタル記録媒体は、記録されるメインデータのうち映像及び／又は音声以外の部分にコピー制限レベルを示すコピー管理情報が付加されており、また前記メインデータのうち映像及び／又は音声の部分に電子透かし情報が付加されており、さらに前記メインデータにエラー訂正コードを追加した後の記録データに特定パターンのエラー情報が意図的に付加されて製造されており、

前記送信側機器は、再生されるディジタル記録媒体を、前記コピー管理情報、前記電子透かし情報、及び前記特定パターンのエラー情報の有無と内容とにより、正当なディジタル記録媒体であるかないかを判断し、前記正当なディジタル記録媒体であると判断された場合は、その記録データを受信側機器へ送信し、

前記受信側機器は、受信するディジタルデータを前記コピー管理情報及び／又は前記電子透かし情報の存否と内容とに応じて再生動作あるいは記録動作の動作制限を行う

ことを特徴とするディジタルコピー制御方法。

【請求項３】

再生または別途記録するためにメインデータが記録されてなるディジタル記録媒体において、

前記メインデータには、映像及び／又は音声以外の部分にコピー制限レベルを示すとともにディジタルコピーを制限する場合ディジタルコピーによって前記コピー制限レベルを強化するように書き替えられるコピー管理情報が含まれ、また、映像及び／又は音声以外の部分にはディジタルコピーによっても書き替えられない電子透かし情報とが外部に読み出し可能な状態で含まれ、

前記メインデータ外には、外部に読み出されない媒体マークが付加され、

これらコピー管理情報、電子透かし情報、および媒体マークは、これら３種類の情報の内容の組み合わせによって前記メインデータの作成者側の意図するところの、媒体再生管理および媒体コピー管理がなされるように構成されている

ことを特徴とするディジタル記録媒体。

【請求項４】

原データにその特徴を損なわない電子透かし情報を付加する透かし情報付加手段と、

原データにコピーを制限するためのコピー管理情報を付加するコピー管理情報付加手段と、

原データに前記電子透かし情報及びコピー管理情報が付加されたメインデータからエラー訂正コードを生成して付加するエラー訂正コード生成手段と、

このエラー訂正コード生成手段でエラー訂正コードが付加されたデータに特定パターンのエラーを媒体マークとして付加するエラー付加手段と

を備えたことを特徴とするディジタル記録媒体作製装置。

【請求項５】

バスを介して接続された複数のディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタルデータを送信するシステムの前記送信側機器として用いられるディジタル再生装置において、

ディジタル記録媒体から記録データを読み出す読出手段と、

この読出手段で読み出された読出データからエラー訂正コードを抽出し、このエラー訂正コードに基づいて読出データの誤りを検出訂正する誤り検出訂正手段と、

この誤り検出訂正手段で検出された誤りが特定パターンであるかないかを検出する特定パターン誤り検出手段と、

前記誤り検出訂正手段で誤り訂正されたデータを前記インタフェースの仕様に合ったディジタル情報の形態で前記バスに出力する出力手段と、

前記誤り訂正されたデータに含まれるディジタルコピーを制限するための電子透かし情報の存否と内容を判定する電子透かし情報判定手段と、

前記誤り訂正されたデータからコピー制限レベルを示すコピー管理情報の存否と内容を判定するコピー管理情報判定手段とを備え、

前記特定パターン誤り検出手段の検出結果に基づいて前記ディジタル記録媒体がオリジナル媒体かコピー媒体かを判定し、この判定結果と、前記コピー管理情報判定手段及び前記電子透かし情報判定手段での判定結果とに基づいて前記送信側機器のデータの再生を許可又は禁止するようにした

ことを特徴とするディジタル再生装置。

【請求項６】
前記コピー管理情報判定手段は、前記コピー管理情報から“コピーフリー”、“１世代コピー可”又は“コピー禁止”の３種類のコピー制限レベルを識別し、
前記電子透かし情報判定手段は、前記電子透かし情報から“コピーフリー”又は“コピー制限付き”の２種類のコピー制限レベルを識別し、
前記特定パターン誤り検出手段は、前記特定パターンの誤りの有無を識別し、
これら各手段での識別結果から正規に記録されたディスクであるかどうかを判定して正規のディスクの場合は再生するようにしたことを特徴とする請求項５記載のディジタル再生装置。
【請求項７】
前記特定パターン誤り検出手段で特定パターンの誤りが検出され、コピー管理情報判定手段で“１世代コピー可”と判定され、且つ電子透かし情報判定手段で電子透かし情報が“コピー制限付き”であると判定された場合、再生動作を実行することを特徴とする請求項６記載のディジタル再生装置。
【請求項８】
前記特定パターン誤り検出手段で特定パターンの誤りが検出された場合で且つ前記コピー管理情報判定手段と前記電子透かし情報判定手段の判定結果が、コピー管理情報が“１世代コピー可”で且つ電子透かし情報が“コピー制限付き”となっている場合を除いて、前記コピー管理情報判定手段と前記電子透かし情報判定手段の判定結果が相矛盾する内容となっているとき、又は前記特定パターンの誤り検出手段で特定パターンの誤りが検出された場合で且つ前記電子透かし情報が検出出来なかった場合、再生を行わないことを特徴とする請求項５又は６記載のディジタル再生装置。
【請求項９】
前記特定パターンの誤り検出手段で特定パターンの誤りが検出されなかった場合で且つ、前記コピー管理情報判定手段と前記電子透かし情報判定手段の判定結果が異なる場合、再生を行わないことを特徴とする請求項５又は６記載のディジタル再生装置。
【請求項１０】
バスを介して接続された複数のディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタルデータを送信するシステムの前記受信側機器として用いられるディジタル記録装置において、
受信したディジタルデータに、“コピーフリー”、“１世代コピー可”又は“コピー禁止”のいずれかのコピー制限レベルを示すコピー管理情報があるかないかをと識別し、在ると識別されたコピー管理情報が“１世代コピー可”であるときはコピー管理情報を“コピー禁止”を示すように書き換えて前記受信したディジタルデータを記録することを特徴とするディジタル記録装置。
【請求項１１】
前記認証された機器には、ディジタル記録媒体に記録されたディジタルデータコンテンツを前記インターフェースを介することなくアナログ信号として出力可能に構成された機器、及び前記インターフェースを介することなくアナログ信号で入力されるデータコンテンツを新たなディジタル記録媒体に記録可能に構成された機器を含み、アナログ信号またはディジタル信号で供給されるデータコンテンツをディジタル記録媒体にディジタル記録する際に、当該媒体上にデータコンテンツに加えて認証された機器間でのみ認証可能な電子認証署名データを記録するように構成されると共に、
ディジタル記録媒体に記録されたディジタルデータコンテンツを再生する際に、当該媒体上に前記認証された機器間でのみ認証可能な電子認証署名データが存在するか否かを検出し、
前記電子認証署名データが存在する場合は当該媒体のディジタルデータコンテンツを再生するように制御される
ことを特徴とする請求項１記載のディジタルコピー制御方法。

【請求項１２】
認証された機器間でのみ認証可能な電子認証署名データが、更に記録されてなる
ことを特徴とする請求項３記載のディジタル記録媒体。
【請求項１３】
認証された機器間でのみ認証可能な電子認証署名データを検出する手段と、電子認証署名データが認証されなかった場合はデータの再生を禁止する手段とを、更に有する
ことを特徴とする請求項５記載のディジタル再生装置。
【請求項１４】
前記認証された機器の少なくとも一部は、ディジタル記録媒体に記録されたディジタルデータコンテンツを前記インターフェースを介することなくアナログ信号として出力可能に構成されており、
これらアナログ信号で供給されるデータコンテンツをディジタル記録媒体にディジタル記録する際に、データコンテンツに加え当該認証された機器間でのみ認証可能な電子認証署名データを当該媒体上に記録するように構成される
ことを特徴とする請求項１０記載のディジタル記録装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００９
【補正方法】変更
【補正の内容】
【０００９】
【課題を解決するための手段】
この発明に係る第１のディジタルコピー制御方法は、バスを介して複数のディジタル機器が接続され、これらディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタル記録媒体からのディジタルデータを送信するに際し、送信側機器が、前記ディジタルデータに含まれるコピー制限のための情報の存否と内容とに基づいて不許可コピーを防止するように、当該送信側機器の再生動作もしくは記録動作の動作制限を行うディジタルコピー制御方法において、本来のディジタル記録媒体は、記録されるメインデータのうち映像及び／又は音声以外の部分にコピー制限レベルを示すコピー管理情報が付加されており、また前記メインデータのうち映像及び／又は音声の部分に電子透かし情報が付加されており、さらに前記メインデータにエラー訂正コードを追加した後の記録データに特定パターンのエラー情報が意図的に付加されて製造されており、前記送信側機器は、再生されるディジタル記録媒体を、前記コピー管理情報、前記電子透かし情報、及び前記特定パターンのエラー情報の有無と内容とにより、正当なディジタル記録媒体であるかないかを判断し、前記正当なディジタル記録媒体であると判断された場合は、その記録データを受信側機器へ送信することを特徴とする。
また、本発明の第２のディジタルコピー制御方法は、バスを介して複数のディジタル機器が接続され、これらディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタル記録媒体からのディジタルデータを送信するに際し、送信側機器あるいは受信側機器が、前記ディジタルデータに含まれるコピー制限のための情報の存否と内容とに基づいて不許可コピーを防止するように、当該送信側機器あるいは受信側機器の再生動作もしくは記録動作の動作制限を行うディジタルコピー制御方法において、本来のディジタル記録媒体は、記録されるメインデータのうち映像及び／又は音声以外の部分にコピー制限レベルを示すコピー管理情報が付加されており、また前記メインデータのうち映像及び／又は音声の部分に電子透かし情報が付加されており、さらに前記メインデータにエラー訂正コードを追加した後の記録データに特定パターンのエラー情報が意図的に付加されて製造されており、前記送信側機器は、再生されるディジタル記録媒体を、前記コピー管理情報、前記電子透かし情報、及び前記特定パターンのエラー情報の有無と内容とによ

り、正当なディジタル記録媒体であるかないかを判断し、前記正当なディジタル記録媒体であると判断された場合は、その記録データを受信側機器へ送信し、前記受信側機器は、受信するディジタルデータを前記コピー管理情報及び／又は前記電子透かし情報の存否と内容とに応じて再生動作あるいは記録動作の動作制限を行うことを特徴とする。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】
また、バスを介して接続された複数のディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタルデータを送信するシステムの前記送信側機器として用いられるこの発明に係るディジタル再生装置は、ディジタル記録媒体から記録データを読み出す読出手段と、この読出手段で読み出された読出データからエラー訂正コードを抽出し、このエラー訂正コードに基づいて読出データの誤りを検出訂正する誤り検出訂正手段と、この誤り検出訂正手段で検出された誤りが特定パターンであるかないかを検出する特定パターン誤り検出手段と、前記誤り検出訂正手段で誤り訂正されたデータを前記インタフェースの仕様に合ったディジタル情報の形態で前記バスに出力する出力手段と、前記誤り訂正されたデータに含まれるディジタルコピーを制限するための電子透かし情報の存否と内容を判定する電子透かし情報判定手段と、前記誤り訂正されたデータからコピー制限レベルを示すコピー管理情報の存否と内容を判定するコピー管理情報判定手段とを備え、前記特定パターン誤り検出手段の検出結果に基づいて前記ディジタル記録媒体がオリジナル媒体かコピー媒体かを判定し、この判定結果と、前記コピー管理情報判定手段及び前記電子透かし情報判定手段での判定結果とに基づいて前記送信側機器のデータの再生を許可又は禁止するようにしたことを特徴とする。

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】変更
【補正の内容】
【００１７】
更に、この発明に係るディジタル記録装置は、バスを介して接続された複数のディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタルデータを送信するシステムの前記受信側機器として用いられるディジタル記録装置において、受信したディジタルデータに、“コピーフリー”、“１世代コピー可”又は“コピー禁止”のいずれかのコピー制限レベルを示すコピー管理情報があるかないかをと識別し、在ると識別されたコピー管理情報が“１世代コピー可”であるときはコピー管理情報を“コピー禁止”を示すように書き換えて前記受信したディジタルデータを記録することを特徴とする。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】変更
【補正の内容】
【００２３】
プレーヤ１は、ＤＶＤ８の再生に先立ち、ディスプレイ装置２及びレコーダ３との間でこれら各機器がコンテンツ作成者の意図どおりに動作する機器であるかどうか相互認証処理を実行する。例えばディスプレイ装置２には、記録機能が無いので、プレーヤ１との間には公開鍵を用いた完全認証が成立する。この場合、記録が禁止されているコンテンツで

も再生が可であればデータが転送される。プレーヤ１とレコーダ３との間は、共通鍵を用いた制限付き認証が成立する。この場合、記録も再生も可であるコンテンツのみがデータ転送される。認証された機器間でのみデータ転送が有効となるように、バス７上のデータは暗号化される。